## Términos y definiciones del Curso 5

A

**Activo:** Elemento percibido como valioso para una organización.

**Agente de amenaza:** Persona o grupo de personas que representa una amenaza intencional para computadoras, aplicaciones o redes.

**Adware:** Tipo de software legítimo o malicioso que se utiliza para mostrar publicidad digital en las aplicaciones.

**Algoritmo:** Conjunto de instrucciones definidas, ordenadas y acotadas para resolver un problema, realizar un cálculo o desarrollar una tarea.

**Algoritmo de cifrado (cipher)**: Algoritmo que cifra la información.  
  
**Amenaza:** Cualquier circunstancia o evento que pueda afectar negativamente a los activos.

**Angler phishing:** Tipo de ataque de suplantación de identidad en el que un agente de amenaza se hace pasar por representantes del servicio al cliente de una empresa en las redes sociales.

**Aplicación potencialmente no deseada (PUA):** Tipo de software que se incluye con programas legítimos y que puede mostrar anuncios, causar la ralentización del dispositivo o instalar otro software no deseado.

**Aprovisionamiento de usuarios:** Proceso de creación, actualización, modificación o eliminación de cuentas o perfiles de usuarios.

**Árbol de ataque:** Diagrama que muestra las amenazas a los activos y cómo se relacionan entre sí.

**Ataque de “agujero de agua” (Watering hole)**: Tipo de ataque en el que un agente de amenaza compromete un sitio web visitado con frecuencia por un grupo específico de usuarios.

**Ataque de caza de ballenas (Whaling):** Tipo de ataque de suplantación de identidad dirigido específicamente a personal de alto rango de una organización.

**Ataque de fuerza bruta:** Proceso de ensayo y error para descubrir información privada, como, por ejemplo, una contraseña.

**Ataque de inyección:** Ataque mediante el cual se introduce un código malicioso en una aplicación vulnerable.

**Ataque de secuencia de comandos en sitios cruzados, o entre sitios, (XSS):** Tipo de ataque de inyección que consiste en insertar código en un sitio web o aplicación web vulnerables.

**Ataque de suplantación de identidad:** (Consultar **Phishing**).

**Ataque XSS almacenado:** Tipo de ataque en el que se inyecta un script o secuencia de código malicioso directamente en el servidor.

**Ataque XSS basado en DOM:** Tipo de ataque en el que se inyecta un código malicioso directamente en la página web que carga un navegador.

**Ataque XSS reflejado:** Tipo de ataque en el que se envía un script malicioso a un servidor que se activa durante la respuesta del mismo.

**Auditoría de seguridad**: Revisión de los controles, políticas y procedimientos de seguridad de una organización.

**Autenticación básica:** Tecnología utilizada para establecer la solicitud de un usuario de acceder a un servidor.

**Autenticación de múltiples factores o multifactor (MFA):** Medida de seguridad que exige a un usuario verificar su identidad en dos o más formas para acceder a un sistema o red.

**Autoridad de numeración de CVE (CNA):** Organización que voluntariamente analiza y distribuye información sobre CVE elegibles.

B

**Bit:** La unidad más pequeña de medición de datos en una computadora.

**Botnet:** Conjunto de computadoras infectadas por software malicioso (malware), que están bajo el control de un solo agente de amenaza, conocido como el “bot-herder”.

C

**Caballo de Troya (troyano):** Software malicioso que parece un archivo o programa legítimo.

**Cargador:** Código malicioso que se inicia después de que un usuario inicia un programa dropper.

**Cebo (Baiting):** Táctica de ingeniería social que incita a las personas a comprometer su seguridad.

**Certificado digital:** Documento electrónico que verifica la identidad del titular de una clave pública.

**Cifrado (encriptación):** Proceso de convertir datos de un formato legible a uno codificado.

**Cifrado asimétrico:** Sistema criptográfico que utiliza dos claves, una pública y otra privada, para cifrar y descifrar datos.

**Cifrado simétrico:** Sistema criptográfico que utiliza una única clave para cifrar y descifrar datos.

**Clasificación de activos:** Práctica de etiquetar los activos en función de cuán sensibles e importantes son para una organización.

**Clave criptográfica:** Secuencia de datos que descifra el texto cifrado o viceversa.

**Colisión de hash:** Situación en la que diferentes entradas comparten el mismo valor hash.

**Controles de acceso:** Tipo de controles de seguridad que gestionan el acceso, la autorización y el manejo de la información.

**Controles de seguridad:** Pautas diseñadas para abordar y eliminar riesgos de seguridad específicos, como la alteración o eliminación de información de perfiles, entre otros.

**Cookie de sesión:** Token que utilizan los sitios web para validar una sesión y determinar su duración.

**Criptografía:** (Consultar **Cifrado**).

**Criptojacking:** Tipo de software malicioso que instala un programa para minar criptomonedas ilegalmente.

**Cumplimiento normativo (Compliance):** Proceso de adherirse y cumplir con las normas y reglamentos internos y externos, con el fin de proteger la información y los sistemas de una empresa.

**Custodio de datos:** Cualquier persona o entidad responsable del manejo, transporte y almacenamiento seguro de la información

D

**Dato:** Información traducida, procesada o almacenada por una computadora.

**Datos en reposo:** Datos a los que no se está accediendo actualmente.

**Datos en tránsito:** Datos que se desplazan de un punto a otro.

**Datos en uso:** Datos a los que está accediendo un usuario.

**Defensa en profundidad:** Estrategia que consiste en usar varias medidas de seguridad en capas para proteger la integridad de la información y reducir el riesgo.

**Día cero:** Vulnerabilidad recién descubierta.

**Dropper:** Tipo de troyano que instala un programa o archivo malicioso en un equipo de destino.

E

**Escáner de vulnerabilidades:** Software diseñado para realizar análisis automáticos de cualquier aplicación, sistema o red en busca de vulnerabilidades.

**Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago (PCI-DSS):** Guía que define controles para la protección de los datos de titulares de tarjetas de pago y otros datos sensibles de autenticación, durante su procesamiento, almacenamiento y transmisión.

**Estándares:** Referencias sobre los objetivos y controles exigibles en lo referente a la seguridad de la información.

**Evaluación de seguridad:** Proceso de verificación que busca determinar la eficacia de las capacidades de ciberseguridad actuales contra las amenazas.

**Evaluación de vulnerabilidades:** Proceso de revisión interna de los sistemas de seguridad de una empresa en busca de posibles debilidades.

**Exploit:** Fragmento de software o secuencia de comandos que se aprovecha de un error o vulnerabilidad.

**Exploits basados en la web:** Fragmento de software o secuencia de comandos que se aprovecha de un error o vulnerabilidad de codificación en una aplicación web.

**Exposición:** Error que puede ser aprovechado por un agente de amenaza.

F

**Función hash:** Algoritmo que produce un código que no se puede descifrar.

**Gestión de activos:** Proceso de seguimiento de los activos y los riesgos que los afectan.

**Gestión de identidad y acceso (IAM):** Conjunto de procesos y tecnologías que ayuda a las organizaciones a administrar las identidades digitales en su entorno**.**

**Gestión de vulnerabilidades:** Proceso de identificar, evaluar y corregir vulnerabilidades.

**Gusano:** Software malicioso que se reproduce por sí mismo y se propaga a través de los sistemas y redes.

H

**Hacker:** Cualquier persona o grupo de personas que utiliza computadoras para obtener acceso no autorizado a los datos. Se diferencia entre hacker ético, que es quien tiene como objetivo mejorar la seguridad y prevenir posibles ataques, y no ético o malintencionado, que es aquel que busca comprometer la seguridad de un sistema informático o de una red, con fines delictivos.

I

**Identificador de sesión (ID de sesión):** Token único que identifica a un usuario y a su dispositivo mientras accede a un sistema**.**

**Información de identificación personal (PII por sus siglas en inglés):** Cualquier información que se pueda usar para deducir la identidad de una persona.

**Información médica protegida (PHI, por sus siglas en inglés):** Cualquier información relacionada con la salud, o la condición física o mental pasada, presente o futura de una persona.

**Infraestructura de clave pública (PKI, por sus siglas en inglés):** Marco de cifrado que garantiza la seguridad del intercambio de información en línea.

**Ingeniería social:** Técnica de manipulación que busca engañar a las personas con el fin de que revelen información o realicen determinadas acciones.

**Inicio de sesión único (SSO):** Solución de autenticación que combina varios inicios de sesión diferentes en uno solo.

**Inventario de activos:** Catálogo de elementos valiosos que se deben proteger.

**Inyección SQL:** Tipo de ataque que consiste en ejecutar consultas maliciosas, con el fin de manipular a una base de datos y acceder a la información.

K

**Kit de phishing:** Conjunto de herramientas de software, preparado para lanzar una campaña de phishing con facilidad.

L

**Lista de vulnerabilidades y exposiciones comunes (CVE®):** Listado de vulnerabilidades y exposiciones conocidas divulgadas públicamente.

M

**Malware sin archivos:** (Consultar **Software malicioso sin archivos**).

**Malware:** (Consultar **Software malicioso**).

**Marco de Ciberseguridad (CSF) del Instituto Nacional de Estándares y Tecnología (NIST):** Marco de adhesión voluntaria creado en los Estados Unidos, que incluye estándares, pautas y prácticas recomendadas para gestionar riesgos para la ciberseguridad.

**MITRE:** Conjunto de centros de investigación y desarrollo sin fines de lucro creado en los Estados Unidos, con el fin de buscar soluciones a posibles amenazas a la ciberseguridad.

**Modelado de amenazas:** Proceso de identificación de activos, sus vulnerabilidades y su exposición a las amenazas, con el objetivo de planificar y optimizar las operaciones de seguridad de la red.

N

**No repudio:** Concepto según el cual no se puede negar la autenticidad de una información.

**Normativas:** Normas establecidas por un gobierno u otra autoridad para controlar la forma en que se hace algo.

O

**OAuth “Open Authorization” (Autorización abierta):** Protocolo de autorización de estándar abierto que comparte el acceso designado entre aplicaciones.

P

**Phishing (Suplantación de identidad):** Uso de comunicaciones digitales en las que se suplanta la identidad de una persona o empresa con el objetivo de engañar a otras personas para que revelen datos confidenciales o implementen un software malicioso.

**Phishing localizado (Spear phishing):** Ataque por correo electrónico malicioso dirigido a una persona o grupo de personas específico que parece provenir de una fuente confiable.

**Política:** Conjunto de reglas que reducen el riesgo y protegen la información.

**Principio de mínimo privilegio:** El concepto de otorgar únicamente el acceso y la autorización mínimos necesarios para ejecutar una tarea o función.

**Privacidad de la información:** Protección contra el acceso y la difusión de datos no autorizados.

**Procedimiento:** Instrucciones paso a paso para realizar una tarea de seguridad específica.

**Proceso de simulación de ataques y análisis de amenazas (PASTA):** Metodología de modelado de amenazas de uso común en numerosas industrias.

**Propietario de datos:** Persona que tiene la potestad de decidir quién puede acceder a su información, editarla, usarla o destruirla.

Q

**Quid pro quo:** Tipo de cebo utilizado para engañar a una persona y hacerle creer que será recompensada si comparte un acceso, información o dinero.

R

**Ransomware:** (Consultar **Secuestro de datos**)**.**

**Recompensas por errores:** Programas que animan a hackers autónomos a encontrar y notificar vulnerabilidades.

**Reforzamiento de la seguridad:** Proceso de reforzar un sistema para reducir sus vulnerabilidades y su superficie de ataque.

**Riesgo**: Cualquier hecho que pueda afectar a la confidencialidad, integridad o disponibilidad de un activo.

**Rootkit**: Software malicioso que proporciona acceso administrativo remoto a una computadora.

S

**Salting (salado):** Protección adicional que se utiliza para reforzar las funciones hash que consiste en añadir un factor aleatorio a cada hash con el fin de que no se pueda predecir.

**Saneamiento de entradas:** Programación que valida las entradas de usuarios y de otros programas.

**Scareware:** Software malicioso que emplea tácticas para asustar a las personas con el fin de que infecten su dispositivo.

**Secuestro de datos (Ransomware):** Ataque malicioso que consiste en cifrar los datos de una organización para exigir el pago de un rescate para restablecer el acceso a ellos.

**Secuestro de sesión:** Ataque malicioso que consiste en obtener el identificador de sesión de un usuario legítimo.

**Segregación de funciones:** Principio según el cuál no se debe otorgar a una misma persona accesos a dos o más responsabilidades dentro del sistema que le permitirían hacer un uso indebido del mismo.

**Seguridad de la información (InfoSec):** Práctica de controlar y salvaguardar los datos de una organización.

**Sentencia preparada (Prepared Statement):** Técnica de codificación que ejecuta sentencias SQL antes de pasarlas a una base de datos.

**Sesión:** Secuencia de solicitudes y respuestas de autenticación básica HTTP de red asociadas con el mismo usuario.

**Sistema de detección de intrusiones (IDS):** Aplicación que monitorea la actividad del sistema y alerta sobre posibles intrusiones.

**Sistema de puntuación de vulnerabilidad común (CVSS):** Sistema de medición que asigna un puntaje a la gravedad de una vulnerabilidad.

**Smishing**: Tipo de ataque de suplantación de identidad (phishing) que utiliza mensajes de texto para engañar a las personas con el fin de obtener información confidencial.

**Software malicioso (Malware):** Programa diseñado para dañar dispositivos o redes.

**Software malicioso sin archivos (Malware sin archivos):** Tipo de software malicioso que utiliza programas legítimos que ya están instalados en una computadora para infectarla.

**Spyware:** Software malicioso que se usa para recabar y vender información sin el consentimiento de su propietario.

**SQL, Structured Query Language (lenguaje de consulta estructurado):** Lenguaje de programación utilizado para crear, interactuar y solicitar información de una base de datos.

**Superficie de ataque:** Suma de vulnerabilidades, vías o métodos susceptibles de recibir un ataque.

T

**Tabla Arcoiris (Tabla Rainbow):** Archivo de valores hash generados previamente y su texto sin cifrar asociado.

**Tabla hash:** Estructura de datos que se utiliza para almacenar y hacer referencia a los valores hash.

**Tailgating:** Táctica de ingeniería social en la que personas no autorizadas siguen a una persona autorizada hasta ingresar a una zona restringida.

**Token de interfaz de programación de aplicaciones (API):** Pequeño bloque de código cifrado que contiene información sobre un usuario.

**Troyano:** (Consultar **Caballo de Troya**).

V

**Vector de ataque:** Vía que utilizan las y los atacantes para penetrar en las defensas de seguridad.

**Virus:** (Consultar **Virus informático**).

**Virus informático:** Código malicioso escrito para interferir en el funcionamiento de las computadoras y dañar los datos y el software.

**Vishing:** Tipo de estafa por suplantación de identidad en la que se busca obtener información sensible a través de una llamada telefónica.

**Vulnerabilidad:** Debilidad que puede ser aprovechada por una amenaza.